ORB
ACADEMIC PUBLISHER

IJCSTA Vol. 1 No. 2, JULY 2014.
ISSN: 2336-0984

International Journal of

Computer Science: Theory and Application

http://www.orb-academic.org/index.php/journal-of-computer-science/

Editorial Board

ORB ACADEMIC PUBLISHER
Available online at www.orb-academic.org
International Journal of Computer Science: Theory and Application
ISSN: 2336-0984
Vol. 1, No. 2, July 2014

The Logical Implication Table in Binary Propositional Calculus: Justification, Proof Automatability, and Effect on Scientific Reasoning

Ahmed Shawky Moussa
Department of Computer Science, Cairo University, Cairo, Egypt
Email: a.moussa@fci-cu.edu.eg

ABSTRACT
Logic is the discipline concerned with providing valid general rules on which scientific reasoning and the resulting propositions are based. To evaluate the validity of sentences in propositional calculus, we, typically, perform a complete case analysis of all the possible truth-values assigned to the sentence's propositional variables. Truth tables provide a systematic method for performing such analysis in order to determine whether the sentence is valid, satisfiable, contradictory, consistent, etc. However, in order to validate logical statements, we have to use valid truth tables, i.e., truth tables that are provably consistent and justifiable by some natural criteria. The justification of the truth table of some logical connectives is straightforward, due to the support of the table in everyday applications. Nevertheless, the justification of one of the logical connectives, namely, the implication operator, has always been difficult to build and understand. Though, the logical implication is arguably the most important operator because of its applications as an inference engine for reasoning in science in general and control engineering in particular. In this paper, the author presents this problem introducing a non-exhaustive proof, which justifies the logical implication's truth table in one phase. The author then proposes another optimal proof, discussing the points of optimization and the effects of the resulting linguistic and philosophical interpretation on the scientific reasoning processes. Finally, the paper envisions possible extension of the proposed methodology to solve similar problems in various types of logic.

KEYWORDS
Logical Implication – Propositional Calculus – Scientific Reasoning.

1. Introduction

Logical reasoning has been the main pillar on which science is constructed. In some times and some cases in history, logical reasoning was the only pillar. The ancient Greek scientists relied almost exclusively on logical reasoning in building their knowledge and formulating their theories, as other scientific methods were not yet technically developed to a satisfactory degree of maturity and reliability. This resulted in a large repertoire of theoretical science, some of which remains to be foundation for sciences and mathematics until today; other turned out to be false philosophical speculations.

The advent of the experimental paradigm of science and its integration with logical reasoning enabled the production of sound science and, to a great extend, clarified the distinction between science and philosophy. Today, computational methods have emerged as the new major paradigm for scientific research, resulting in the classification of the scientific endeavors into three main categories: theoretical, experimental, and computational science.

Regardless of the choice of methodology, logical reasoning and mathematical logic remain to be the cornershotnes for all the three main paradigms. After all, computation, at the bottom, is automated logical reasoning and mathematical models and techniques are tools for formulating and quantifying the reasoning process.

The above introduction signifies the importance of forming, producing, and validating logical propositions in science. The validation process involves the evaluation of the validity of sentences in propositional logic, which, in turn, involves the evaluation of the statement's truth function under all possible interpretations. For example, a proposition P is said to be *valid*, also called a *tautology*, if it is evaluated to be true under every possible interpretation of P. On the other hand, P is said to be *contradictory* if it is false under all possible interpretations. In between the two extremes, there are different degrees of validity leading to evaluating the sentence as *satisfiable*, *consistent*, etc. [1].

The validation process requires a complete analysis of all the possible truth-values under all possible interpretations of the

proposition to construct the truth function for that proposition. This is typically performed by constructing truth tables, which list all the possible truth-values for the proposition currently under evaluation [2]. The use of truth tables is an important outcome of the development of the theory of symbolic logic, which was initiated by George Boole [3], who formulated the logic of Aristotle as algebra of classes [4], [5]. The integration of symbolic logic with the semantic theory of logic resulted in mathematical logic and propositional calculus, which have had significant effect on the development of science in general and the information and computation theories in particular.

This section provided the necessary background for the current paper, signifying the necessity of a sound validation process for logical propositions, which are the building blocks of science and knowledge. The next section presents the particular problem of justifying the logical implication table, states a possible disadvantageous solution, and provides motivation for the need for new proofs. Section three includes the author's presentation of an unpublished proof by Dr. Stephen Leach of Florida State University based on the requirement specified by R. L. Goodstein [6]. In section four, the author introduces his new automatable proof based on incremental constructive reasoning. Section five, then, includes a comparison between the two proofs pointing out how the latter is advantageous over the other proofs. Section six discusses the linguistic, philosophical, and scientific implications and consequences of the table. Finally, section seven concludes the paper and provides pointers to possible future follow up research.

2. The Research Problem

The truth tables for many logical connectives used in constructing compound propositions seem justifiable and easy to accept, even without a mathematical proof. They simply go with the natural intuition and make sense in daily applications. Propositional connectives that fall into this category are the *negation* operator (*NOT* connective, denoted as $\neg$), the *conjunction* operator (*AND* connective, denoted as $\wedge$), and the *logical equivalence*, also known as the *biconditional*, operator ($\Leftrightarrow$) – that is the $if-and-only-if$ form (*iff*). The *disjunction* operator (*OR* connective, denoted as $\vee$) may seem a little more problematic until the type of the intended disjunction, *exclusive* or *inclusive*, is determined. Once this determination is made, the problem disappears. However, one propositional connective, namely the *logical implication* ($\Rightarrow$), also known as the *conditional* operator and the $if-then$ form, has always been harder to justify and understand. Goodstein explains this exceptional difficulty by arguing that the "everyday usage [of the $if-then$ form] is inadequate to determine the table for [the logical] implication since it serves only to tell us that a true sentence does not imply a false one, but is silent on the question of what is implied by a false sentence" [6]. The truth table for the logical implication is illustrated in Table 1. In the table, P and Q are sentence variables, 1 represents *true*, and 0 represents *false*.

It is important here to note that the current treatment of the $if-then$ form is only concerned with the truth function of the resulting compound proposition. A compound sentence is considered to be *truth-functional*, only if the truth-value of the sentence is a function of the truth-value of its constituent sentence variables

Table 1. *Truth table for logical implication.*

P	Q	$P \Rightarrow Q$
1	1	1
1	0	0
0	1	1
0	0	1

[7]. It is needless to say that the everyday use of the $if-then$ form is not limited to the truth- functional applications.

Even after we limit our discussion to the truth-functional $if-then$ statements, when we look at Table 1, we see that each cell in the third column could have been assigned any one of the two values, 0 or 1, i.e., false or true, respectively. With four rows representing all the possible combinations of the sentences P and Q, then Table 1 is one of a total of $2^4 = 16$ possible tables. Now we find ourselves obligated to answer the question: why should we believe that this table is the right one? The necessity of answering the question is further amplified by the fact that the resulting linguistic implication of the compound proposition may not be so obvious or supported by the natural and intuitive everyday usage of the sentence form.

Let us present the problem further by a concrete example. Let the sentence variable P stands for the proposition "electromagnetic waves travel in the void", and let Q represents the sentence "the ether exists". Now, the compound proposition $S_1 = P \Rightarrow Q$ stands for "if electromagnetic waves travel in the void, then the ether exists". Let us also consider the compound proposition $S_2 = \neg P \Rightarrow \neg Q$, which represents the proposition "if electromagnetic waves do not travel in the void, then the ether does not exist". According to Table 1, the statement S_1 is false but S_2 is true. This is not an obvious conclusion to many people. Both propositions include one true and one false statement. In S_1, the antecedent is true and the consequence is false while S_2 is vice versa.

Although the logical implication operator is the most controversial among logical connectives, it is arguably the most important in science and engineering applications. The additional importance of the conditional connective is attributed to two sources. Firstly, it is inherently the building block for scientific reasoning and the inference mechanisms necessary for constructing proofs and drawing conclusions. A comprehensive look at how the modern science developed at the dawn of the twentieth century reveals a development pattern where the outcome of experiments is used as the antecedent for an $if-then$ – i.e., a logical implication – statement. The consequence of the $if-then$ form comes then as a new theory, model, proposition, or even a postulate, or set of postulates, that would lead later to a new scientific discovery. This is how we established the fact that light waves are electromagnetic waves and the fact that electromagnetic waves travel in the void as a consequence of the outcome of Michelson-Morley experiment. It is also how the special theory of relativity based on the universality of the laws of physics and the speed of light evolved. Similarly was the rational for the development of quantum mechanics, the series of models for the atomic structure, the De Broglie's hypothesis, and many other discoveries that redefined the modern science. They all

were compound propositions of the "*if P then Q*" form ($P \Rightarrow Q$ in symbolic notation) with different degrees of complexity. If we take P to be the outcome of the experiment of Hans Geiger and Ernest Marsden and Q to be the Rutherford model of the atom, we get one of the most famous examples of the dependence of science on the above reasoning process in the $if - then$ form [8]. Secondly, among all the logical operators, the $if - then$ form is of exceptionally intensive and extensive use in system control theory and applications. Many control systems, regardless of the type of logic they utilize, rely on the automation of a set of $if - then$ rules for adaptive system control [9].

This discussion of the merits and criticality of the logical implication makes it clear that it is of fundamental necessity that the controversy about the $if - then$ sentence form be solved preferably through a solid mathematical proof, since obviously other tools are not adequate or sufficient. The necessity here is not for specialized logicians. The need is rather for students to understand, applied scientists to use, and automated reasoning practitioners to program.

A rather naïve way to prove the correctness of Table 1 is to generate all the possible sixteen tables and systematically prove by contradiction the invalidity of each and every one of them, except the one represented by Table 1. This would be a tedious and very lengthy proof, which, consequently, would not contribute significantly to the realization of the linguistic and philosophical implications and the practical applications of Table 1. The next two sections present alternate proofs to this exhaustive search methodology. Both proofs assume that the tables for all other logical operators are correct and can be used. Table 2 represents the table for the logical conjunction operator since it will be particularly used in both proofs.

Table 2. *Truth Table for Logical Conjunction.*

P	Q	$P \wedge Q$
1	1	1
1	0	0
0	1	0
0	0	0

3. A Proof by Incremental Constructive Reasoning

This proof was proposed by Dr. Stephen Leach at Florida State University in the late 1970's. The proof is unpublished and the current presentation and mathematical formulation of the proof are made by the author. Leach's proof is based on the criteria set by Goodstein [6], which states that a valid logical implication table must preserve two properties, that is, it must be *transitive* and *non-commutative*. Based on these criteria, Leach uses his own mathematical logical formula to incrementally construct the table, one row at a time, showing, in one phase, that Table 1 is the only table that can be constructed without having to visit all or any of the other fifteen tables.

The proof

In order for the table to be transitive, we want the proposition Prop (1) below to be a tautology.

Prop (1)

$$[(P \Rightarrow Q) \wedge (Q \Rightarrow R)] \Rightarrow (P \Rightarrow R)$$

The proposition Prop (1) being a tautology means, in words, that if P always implies Q and Q always implies R, then we can conclude that P always implies R. The non-commutability property means that $P \Rightarrow Q$ and $Q \Rightarrow P$ and cannot have the same truth-value. This is important because if they do, the logical implication ($\Rightarrow$) becomes a logical equivalence ($\Leftrightarrow$). Using these two properties and assuming the correctness of the other truth tables, Leach proceeds to justify the logical implication table, starting by proving the last row of Table 1 by contradiction as follows:
Suppose the last row of the table was as follows, in contradiction with Table 1:

P	Q	$P \Rightarrow Q$
0	0	0

If we substitute Q for R in Prop (1) we get

Prop (2)

$$\{[(P \Rightarrow Q) \wedge (Q \Rightarrow Q)] \Rightarrow (P \Rightarrow Q)\} = 1$$

[*] $\because (P \Rightarrow Q) = 0$ by the contradictory assumption,
[†] $\therefore \{[0 \wedge 0)] \Rightarrow 0\} = 0$ by substituting 0 for each direct implication in Prop (2),
$\therefore \{0 \Rightarrow 0\} = 0$ by substituting from the fourth row of Table 2, but this contradicts with Prop (2) = 1 and the requirement that Prop (1) is a tautology. Then, the contradictory assumption is incorrect and the fourth row of Table 1 is correct.

$$\therefore 0 \Rightarrow 0 = 1 \tag{1}$$

Now, $\because (0 \Rightarrow 0) = 1$ and since Prop (1) is a tautology,
$\therefore \{[(0 \Rightarrow 0) \wedge (0 \Rightarrow 0)] \Rightarrow (0 \Rightarrow 0)\} = 1$
$\therefore \{[1 \wedge 1] \Rightarrow 1\} = 1$ by substituting from (1)
$\therefore \{1 \Rightarrow 1\} = 1$ by substituting from the first row of Table 2. This proves the first row of Table 1.
This proves the first row of Table 1.

$$\therefore 1 \Rightarrow 1 = 1 \tag{2}$$

Now, by the second property of the table as required by Goodstein to be non-commutative, $(1 \Rightarrow 0)$ and $(0 \Rightarrow 1)$, which are the second and third rows of the table, cannot have the same truth-values. Then, from the second and third row of Table 2 for the logical conjunction we get,

Prop (3)

$$\{(1 \Rightarrow 0) \wedge (0 \Rightarrow 1)\} = 0$$

Since Prop (1) is a tautology, it should be true regardless of the truth-values assigned to P, Q, and R. Then we are justified when

[*] $\because$ is symbolic notation for "since".
[†] $\therefore$ is symbolic notation for "then".

we pick any combination of truth-value assignments. Hence, we consider the case when $P = 1$, $Q = 0$, and $R = 1$.
$\therefore \{[(1 \Rightarrow 0) \wedge (0 \Rightarrow 1)] \Rightarrow (1 \Rightarrow 1)\} = 1$ since Prop (1) is a tautology.
$\therefore \{(0 \Rightarrow (1 \Rightarrow 1)\} = 1$ from Prop (3).
$\therefore \{(0 \Rightarrow 1\} = 1$ by application of (2), and this proves the third row of Table 1.

$$\therefore 0 \Rightarrow 1 = 1 \tag{3}$$

Now, by the non-commutability property, rows two and three of Table 1 must have different truth-values.

$$\therefore 1 \Rightarrow 0 = 0 \tag{4}$$

By (1), (2), (3), and (4), Table 1 is justified and complete.

4. Alternate Automatable Proof

In this section, the author proposes a different proof, which is still based on incremental constructive reasoning. Although the above proof indeed inspired the new one, but the author developed the new proof in an attempt to achieve three additional advantages:

1. Increased simplicity. The fundamental idea of both proofs is to build on some natural criteria to which we want the logical implication table to conform. However, the simpler the criterion form and structure, the easier it is to understand the table and its applications. After all, the logical implication is not meant to be used only by mathematical logicians.

2. Better systematic autonomy. Although relying on selected natural criteria for justification has the advantage of providing support and acceptability for applications in reasoning processes of any field, but we hope the proof itself is systematically automatable. This would have the advantage of the proof being programmable into autonomous reasoning and inference systems.

3. Self-evolution and self-evidence. Although the previous proof followed incremental constructive reasoning to justify the table one row at a time, it started by assuming the existence of the table. This does not invalidate the proof itself. However, it poses a big obstacle to achieving full autonomy of the proving mechanism, since it does not answer the question of how we generated the table to start with. It seems to be subjectively selected from the sixteen possible ones. A proof that generates the table from scratch in a self-evolutionary self-evident manner would definitely be a big plus from the points of credibility, simplicity, and automatability.

The Proof

The logical implication table, to be correct, is expected to satisfy the following two conditions:

- 1. For any two sentence variables P and Q, we want the following proposition Prop (4) to be a tautology [1].

Prop (4)
$(P \wedge Q) \Rightarrow P$

- 2. As required by Goodstein, the table is non-commutative, that is $P \Rightarrow Q$ and $Q \Rightarrow P$ cannot have the same truth-value for all P and Q [6].

The first condition is necessary to maintain the compatibility with the logical conjunction table, Table 2. The second is to distinguish the logical implication from the logical equivalence, as explained in the previous proof. Then, the reasoning process proceeds as follows:

Since proposition Prop (4) is a tautology, $(P \wedge Q) \Rightarrow P$ is true, regardless of the truth-values of $P \wedge Q$ and P. Then we consider all the possible cases for $P \wedge Q$. We have two cases: Case 1: $P \wedge Q = 1$ and Case 2: $P \wedge Q = 0$.

Case 1: $P \wedge Q = 1$ *iff* $P = 1$ and $Q = 1$ from Table 2.
$\therefore [(1 \wedge 1) \Rightarrow 1] = 1$ since the proposition is a tautology.
$\therefore (1 \Rightarrow 1) = 1$ from the first row of Table 2. This is the case of row number one of Table 1 and we encode it into a new table, Table 3. To follow the evolution of the table, we encode one phase of the table at a time with the table number as Table 3–*i*, where *i* represents the number of rows filled to the current phase.

Table 3.1. *Logical implication table with one row.*

P	Q	$P \Rightarrow Q$
1	1	1

Case 2: $P \wedge Q = 0$. According to Table 2, this can happen in any one of three subcases:

Case 2.1: when $P = 1$ and $Q = 0$.
$\therefore [(1 \wedge 0) \Rightarrow 1] = 1$ since the proposition is a tautology.
$\therefore [0 \Rightarrow 1] = 1$ from the second row of Table 2. This is the case for row number three of Table 1. Then we have the first and third rows thus far as in Table 3–2.
Case 2.2: when $P = 0$ and $Q = 1$.
$\therefore [(0 \wedge 1) \Rightarrow 0] = 1$ since the proposition is a tautology.
$\therefore [0 \Rightarrow 0] = 1$ from the third row of Table 2. This is the case for row number four of Table 1. Then we have rows number 1, 3, and 4 thus far as in Table 3–3.

Case 2.3: when $P = 0$ and $Q = 0$.
$\therefore [(0 \wedge 0) \Rightarrow 0] = 1$ since the proposition is a tautology.
$\therefore [0 \Rightarrow 0] = 1$ from the fourth row of Table 2. However, this does not produce any new result but the redundant outcome asserts the case of row 4 in Table 3.

Table 3.2. *Logical implication table with two rows.*

P	Q	$P \Rightarrow Q$
1	1	1
0	1	1

Table 3.3. *Logical implication table with three rows.*

P	Q	$P \Rightarrow Q$
1	1	1
0	1	1
0	0	1

Now, by the non-commutability property, $(P \Rightarrow Q)$ and $(Q \Rightarrow P)$ cannot have the same truth-value for all P and Q. Since P and Q have the same truth-value in rows number 1 and 4, then row number 2 must be different from row number 3.
$\therefore (0 \Rightarrow 0) = 1$ in row number 3,
$\therefore (1 \Rightarrow 0) = 0$ is the only choice for row number 2 and this completes Table 3.

Table 3.4. *The Logical implication table complete.*

P	Q	$P \Rightarrow Q$
1	1	1
1	0	0
0	1	1
0	0	1

Now, Table 3 is complete and perfectly matches Table 1.

5. Comparison and Assessment

As stated above, the author attempted devising the latter proof hoping to achieve three objectives, which would be three points of improvement over the first proof. The first objective was to aim at increased simplicity. This was implemented in the second proof by building on a simpler tautology than the ones used by Goodstein or Leach. Proposition Prop (4) is obviously simpler than Prop (1) and involves smaller number of variables – two rather than three. The second objective of the author's proof was to attempt to achieve better systematic autonomy. This means to minimize the subjective involvement in the justification process. In the first proof, in order to prove the third row in (3), we subjectively selected one case out of $2^3 = 8$ cases, that was the case when $P = 1$, $Q = 0$, and $R = 1$. The alternative to this subjective interference in the proving process was to consider all the possible cases, eight of them. The outcome would still have been the same, but the proof would have been much longer and the results would have been too redundant. Hence, we had to choose between extreme redundancy and subjective interference. On the other hand, in the second proof, there was no need for subjective intervention at all, and we still had only one redundant evaluation, which served to assert the fourth row of the table without producing new results. Unlike carrying on seven redundant evaluations, this is obviously an acceptable computational cost for autonomy implementation.

Finally, Leach's proof pre-assumed the existence of the logical implication table, Table 1. The task then was to prove the correctness of the table by contradiction if the fourth row was set differently. However, while this does not disqualify the proof, it does not indicate how Table 1 was selected among sixteen possible tables either. In contrast, the author's proof did not pre-assume the existence of any table. Rather, it systematically generated the table from scratch. This leads to not only full objective autonomy eliminating any subjective intervention, but also a self-evolutionary and self-evident table. This was the last objective of the author to produce a simpler, more credible, and fully authomatable proof.

6. Usage, Applications, and Further Justification

Although the proofs above justify the truth table for the logical implication connective, some background in mathematical logic, admittedly at a certain level, is required not only to generate the proofs but also to understand them. Understanding the logical, linguistic, and philosophical applications of other logical operators may not necessarily require such a background. Let us take the table for the logical *AND*, Table 2 above, for example. According to this table the statement $(P \wedge Q)$ can be true only when both P and Q are true. This is why $(P \wedge Q) = 1$, i.e., true, in the first row and is false, 0, otherwise. In words, this is not difficult to understand or explain even to audience without mathematical background. It simply states that if P and Q stand for simple sentences, then the compound statement "P and Q" would be true only when both "P" and "Q" are true. For instance, if "P" = "today is sunny", and "Q" = "today is a holiday", then the statement $(P \wedge Q)$ would be true only if today is both sunny and a holiday. The truth of one of the two is not sufficient to make the statement true, and the falsity of just one of them is sufficient to make the statement false. Explaining the disjunction, *OR*, table can be done similarly without the use of mathematics, after the type of the disjunction is selected, that is exclusive or inclusive *OR*.

But what about the $if - then$ table, can we explain it in words in a similar manner without using mathematical logic? The author contends that the answer is: yes, we can, but we have to admit that it would not be as easy as it is in the cases of *AND*, *OR*, and *NOT*. A minimum level of sophistication is needed to understand the linguistic interpretation of the logical implication table. Here is a proposed way of explaining and applying it, first to the general audience and then to the scientific community.

Let us take the case "P" = "the sun rises in the east", and "Q" = "the Giza pyramids are in Egypt". According to Table 1, since P is true and Q is true, the "$P \Rightarrow Q$" = "if the sun rises in the east then the Giza pyramids are in Egypt" is true, which is obvious; a true condition leading to a true conclusion makes a true statement, even when the condition and conclusion seem unrelated, after all we are analyzing the truth functional statement. Now, let us take row 2 and make Q false by replacing it with $\neg Q$. Then row 2

states that the statement "$P \Rightarrow Q$" = "if the sun rises in the east then the Giza pyramids are not in Egypt" is false. This should be obvious too because we have a true condition that leads to a false conclusion, which would be against our knowledge of the current world where we live. As for rows 3 and 4, let us make "P" false by replacing it with its negation "$\neg P$". Then rows 3 and 4 say that "$\neg P \Rightarrow Q$" = "if the sun does not rise in the east then the Giza pyramids are in Egypt" is a true statement, and that "$\neg P \Rightarrow \neg Q$ " = "if the sun does not rise in the east then the Giza pyramids are not in Egypt" is also a true statement. This simply is saying that if the sun does not rise in the east then any conclusion can be considered true. This is because if the sun does not rise in the east, then we would be in a different world where we do not know if the Giza pyramids are in Egypt or not. In fact, in that case, would not even know if the pyramids or Egypt would exist at all. Then it is safe to assume that any conclusion is true in that case.

In the example above, the falsity of the antecedent of the conditional statement led to a completely different world where we would not know the correct conclusion and assumed that by default any conclusion could lead to a true statement. However, the antecedent of a conditional statement does not always have to be so fundamental to our world like the sun rising in the east, which renders its negation as such unrealistic philosophical hypothesis. Sometimes the falsity of the antecedent is the result of wrong, or lack of, information. Furthermore, the truth and falsity of the antecedent, or the consequence, may change over time, but this still would not change the validity of the logical implication table. For example, at one point in time, our assumption of the existence of the ether was solely based on logical reasoning in the *if – then* form in the absence of any experimental or observational evidence in support or denial of the proposition. If light is electromagnetic waves, then the ether must exists. This was based on another assumption that waves must travel in a medium. However, since Michelson and Morley discovered the non-existence of the ether, we flipped the antecedent and the consequence in the conditional statement to state that "if there is no ether, then electromagnetic waves can travel in the void". However, the author contends that the argument in the previous paragraph still holds because a change in our knowledge of the world is equivalent to a change in the world itself. If what we knew turns out to be incorrect, then this is equivalent to knowing a different world. In both cases we reasoned about a hypothesis that never existed. The only difference between the two cases is that when we reasoned about the sun not rising in the east, we reasoned about an unrealistic assumption if it occurs in the future, while with the case of the ether we reasoned about an unrealistic assumption that we mistakenly thought was realistic in the past. To demonstrate this idea, let us take the same proposition we ended up with in the above example: "if there is no ether, then electromagnetic waves can travel in the void". Now we know that this statement is true because both the antecedent and the consequence of the conditional statement are both true. But what if we discover one day that the ether actually exists, would the truth of the same whole compound statement be reversed then? In that case, the antecedent, i.e., "there is no ether" becomes false, which according to Table 1 makes the whole statement still true regardless of the truth-value of the consequence. This is in perfect agreement with the argument above about a different world where the sun does not rise in the east. In both cases the statement was made about a different world that has not been known in the first example, and was thought incorrectly to be known in the latter.

Now, one serious argument can be raised against the interpretation above, that is, on rows 3 and 4, if the falsity of the condition means that we simply do not know the conclusion, why is it the case that we assume both to be true? Why not assume both to be false instead? The author's answer to that question is that the default choice of the truth of the proposition is consistent with the assumption that when the antecedent is false then we do not know the consequence and hence all consequences are possible. If one consequence makes the statement false, this would be as if we are stating the impossibility of that consequence. This would be against the natural conclusion that all the consequences are possible when the condition is false, which means that we are dealing with a different, or unknown, world. Normally in science, we assume all outcomes are possible unless we have evidence or reason to believe that some consequence is impossible. Therefore, the default setting of the proposition to be true, rather than false, when the antecedent is false is supported by some natural criteria.

For a concrete example of this approach, let us consider reasoning process about *String Theory*. We all know today that although string theorists have some mathematical evidence and basis for the theory, the skeptics argue that we have no way today, or in the foreseen future, to test the string theory. Hence, string theorists are building arguments on unverifiable science, which renders all consequences possible. Thus far, this deduction is in agreement with the above interpretation of the logical implication. Nevertheless, without taking sides on the string theory, the author wants to use a reasoning process about the theory to prove the point of the above interpretation of Table 1. Therefore, we consider the case when "P" = "the string theory is confirmed", which both the advocates and the skeptics agree is a false statement, taking into account the fact that 'confirmed' means tested methodically and found to be verifiable and applicable. Now, let us take the case of "Q" = "the quantum theory is correct", which we all agree is a true statement according to our knowledge today. Then let us consider the two propositions $(P \Rightarrow Q)$ and $(P \Rightarrow \neg Q)$. The first proposition states that "*if* the string theory is confirmed the quantum theory is correct", while the second proposition states that "*if* the string theory is confirmed the quantum theory is incorrect". The author argued above that it is safe and natural to assume both these propositions to be true, which is in accordance with the fact that all conclusions are possible since P is false. Indeed, setting either, or both, of the above two propositions to be false, implies that we have knowledge or evidence of the impossibility of some consequence of the confirmation of string theory. This surely contradicts with the assumption that P is false. Otherwise, the implied knowledge or evidence could be taken as a confirmation of the theory, which would make P a true statement.

The above linguistic interpretation is also asserted by the fact that logical implication $P \Rightarrow Q$ is logically equivalent to the logical disjunction $\neg P \vee Q$. Both statement forms have the same truth table. This implies that one can be taken as a way of looking

at the other. The logical equivalence between the two implies that for the "*if P then Q*" to be true, *P* must be false, or *Q* must be true. When *P* is false, the statement will be true regardless of the truth-value of *Q*. When *Q* is true, the statement will be true regardless of the truth-value of *P*. This goes in perfect agreement with the preceding linguistic interpretation.

7. Conclusion and Future Vision

It is possible to justify the logical implication table of propositional calculus without having to perform exhaustive search of all possible sixteen tables. This paper presented two methods of proof by incremental constructive reasoning: one is an unpublished proof by Dr. Stephen Leach of Florida State University, and one made by the author. In each proof, one row of the table is either proved – as in the first proof – or generated – as in the second. Once a row is proven or generated, it can be used to generate another, which in turn is used again until the entire table is constructed in one phase as a single solution with no alternatives. The author devised the second proof to achieve three objectives: develop a simpler proof, implement full autonomy, and build a self-evolutionary, self-evident table.

The logical implication is of great importance in all types of logic because of its use in scientific reasoning and developing inference and control systems. Hence, a systematic method of justification based on defined natural criteria is essential to the understanding, functionality, and utilization of the table. The development of the second proof contributes to the understanding of the linguistic interpretation of the table. In addition, the resulting automatable proof is necessary for designing logical systems and computing with words

Acknowledgments

The author wishes to thank Dr. Stephen Leach for his permission to use his unpublished proof in this paper. The author also wishes to acknowledge that Dr. Leach's proof inspired the author and without it a new proof by the author may have not been possible. The author acknowledges that both proofs were produced at the mathematical logic class of Professor Hilbert Levitz and under his guidance. Finally, the author thanks Professor Michael Kasha and the Department of Chemistry and Biochemistry at Florida State University for their tremendous support and funding of this research.

References

[1] MENDELSON, Elliot. *Introduction to Mathematical Logic*. Chapman & Hall, 1997.

[2] MANNA, Zohar, WALDINGER, Richard. *The Logical Basis for Computer Programming*. Vol. 1: Deductive Reasoning. Addison-Wesley, 1985.

[3] ROUVRAY, Dennis. *Fuzzy Logic in Chemistry*. Academic Press 1992. p. 19-20.

[4] BOOL, George. *An Investigation of the Laws of Thought*. Walton and Maberley 1854. Cited in [3], [6].

[5] BOOL, George. *The Mathematical Analysis of Logic*. 1847. Cited in [6].

[6] GOODSTEIN, R. L. *Development of Mathematical Logic*. Springer-Verlag 1971. p4.

[7] BAKER, Stephen. *The Elements of Logic*, 4th Ed. McGraw-Hill 1985. pp. 100 - 107.

[8] KRANE, Kenneth. *Modern Physics*, 2nd Ed. John Wiley and Sons 1996.

[9] KLIR, George, YUAN, Bo. *Fuzzy Sets and Fuzzy Logic: Theory and Applications*. Prentice Hall 1995.

ORB ACADEMIC PUBLISHER

Available online at www.orb-academic.org

International Journal of
Computer Science:
Theory and Application
ISSN: 2336-0984

Vol. 1, No. 2, July 2014

Random Keying Technique for Security in Wireless Sensor Networks Based on Memetics

S.B. Suman[1], P.V. Ranjith Kumar[2], E. Sandeep Kumar[3]

[1] *Dept. of Computer Science & Engg, M S Ramaiah Institute of Technology, Bangalore, Karnataka, India.*
[2] *Dept. of Electronics & Communication Engg, M S Ramaiah Institute of Technology, Bangalore, Karnataka, India.*
[3] *Dept. of Telecommunication Engg, JNN College of Engineering, Shimoga, Karnataka, India.*
Email: sandeepe31@gmail.com

ABSTRACT
Wireless Sensor Networks (WSNs) are often prone to risk of security attacks and vulnerabilities. This is because of the less human intervention in their operations. Hence, novel security mechanisms and techniques are of a prime importance in these types of networks. In this context, we propose a unique security scheme, which coalesce the random keying technique with memetics. The application of these kinds of bio-inspired computation in WSNs provides robust security in the network with the obtained results supporting the security concerns of the network.

KEYWORDS
Random Keying Technique — Memetics — Bio-Inspired Computation.

1. Introduction

Wireless sensor networks is gaining lot of research interest in the present scenario because of its vast and versatile applications. These networks are of great requirements in remote monitoring and military applications where they exchange sensitive data. Security is an area that has been a challenge for the researchers. This is due to the versatility and complexity in attacks to which these networks are often prone. Hence, in this paper we propose a random keying technique merging with the concepts of memetics to combat against the spoofing attacks in the network. Spoofing is a type of attack where the adversary tries to impinge unwanted or false information packets into the network to hamper its normal operation. Few researches have been carried out in solving the issues of WSNs using memetics.

Chuan- Kang Ting et al. [1] propose a scheme for improving the network lifetime by enabling more coverage using memetic algorithm for WSNs. Konstantinos et al. [2] propose a method for improving network lifespan using memetic algorithm as an improvement on the genetic algorithm, taking into accounts of communication parameters and overheads of the sensor nodes. Sandeep et al. [3] propose a novel biologically inspired technique that uses random keying technique with the concepts of artificial immune system for identifying the spoofing attacks in the network. Sandeep et al. [4] propose a bio-inspired approach for addressing node capture attack, which is a combination of artificial neural networks with the game theory as a combat mechanism against malicious attacker. Kashif et al. [5] propose a bio-inspired approach that uses Ant Colony Optimization (ACO) for routing, and artificial immune system for securing from abnormalities and routing attacks. Rongrong Fu et al. [6] developed a bio- inspired security framework that adapts Artificial Immune System (AIS) with the fuzzy techniques for detecting anomalies in the network. Ranjith et al. [7] proposed a bio-inspired security technique, which is based on genetics as counter measure against spoofing attacks.

According our knowledge, very few research works has been carried out using memetics in solving issues of WSNs and with respect to applications of memetics concept is a novel approach towards security. In the proposed work, we use a combination of random key distribution scheme with memetic concepts for providing robust security for WSNs. The algorithm was simulated in MATLAB and the results prove that the method is energy efficient compared to the other widely used cryptographic techniques like ECC and RSA, while combating against spoofing attacks.

The rest of the paper is organized as follows: section 2 deals with memetics, section 3 with the proposed methodology, section 4 with radio model, section 5 discusses the attack scenario, section 6 deals with the simulations, section 7 deals with the results and discussions, section 8 with the concluding remarks of the paper and finally the paper ends with few references.

2. Memetics

Memetics is a theory based on Darwinian evolution, originating from the popularization of Richard Dawkins book ‘the selfish gene’. A ‘meme’ is same as ‘gene’ and but these are termed as ‘units of culture’, which are “hosted” in the minds of one or more

individuals, and which can reproduce itself, thereby jumping from mind to mind [8]. The concept of 'memetics' has been developed as 'memetic algorithm', for solving optimization problems.

2.1 Memetic algorithm

Memetic algorithms have elements of Metaheuristic and Computational Intelligence. Although they have principles of evolutionary algorithms, they may not strictly be considered an evolutionary technique. Using ideas of memes and memetic algorithms in optimization may be referred to as memetics computing [9]. Ideally, memetic algorithms embrace the duality of genetic and cultural evolution, allowing the transmission, selection, inheritance, and variation of memes as well as genes. The memetic algorithm can simply be considered as the improvement over the genetic algorithm in the notion that, the genes are transferred directly to the individual but the memes are processed locally and then transferred. Hence, adding local search to the genetic algorithm results in memetic algorithm.

The algorithm is given below:

1. **Start**: Randomly generate a population of N chromosomes.

2. **Fitness**: Calculate the fitness of all chromosomes.

3. Create a new population:

   – **Selection**: According to the selection criteria, select two chromosomes from the population that are best chromosomes.
   – **Crossover**: Perform crossover on the two chromosomes selected.
   – **Local search**: search for the best chromosomes.
   – **Mutation**: Perform mutation on the chromosomes obtained with small probability.

4. **Replace**: Replace the current population with the new population.

5. **Test**: Test whether the termination condition is satisfied. If so, stop. If not, go to Step 2.

This algorithm is modified for providing security in the WSNs.

3. Proposed Methodology

This section deals with the method introduced in the regard of providing security in the network.

3.1 Random Key range distribution

3.1.1 At the Base Station (BS) - Set up phase

i - Set the range with in which the keys have to be selected. The keys (integer numbers) between these ranges are the initial set of populations (memes). Let this be (A,B).

ii - From the range (A,B) a random set of keys will be selected for scaling down the range, this indicates the optimal set of the keys, which participate in the further process. Let this be (X,Y), where X is the lower limit and Y is the upper limit.

iii - Within (X,Y), randomly two numbers will be picked, and sent to the Cluster Head (CH). Step iii is repeated until all the CHs receive two random numbers from the BS. Let the number received at the CHs be (p,q), where, p is the lower limit and q is the upper limit.

3.1.2 At the Cluster Heads

The received range from the BS will be sent all the member nodes of its cluster. This is (p,q), which is dealt in the previous section.

3.2 Steady phase communication

1. Ordinary member node, if it wants to communicate with its CH, it randomly picks two numbers from within the range (p,q). The numbers (keys) in the range (p,q) is the pool of population of memes. The chosen numbers in this pool indicates the best locally picked memes for the further processes. Let this be (m,n).

2. These memes are allowed to crossover with each other. The procedure of the crossover is dealt in the later sections of the paper.

3. The crossovered numbers (memes) are now checked for fittest candidate, for the further mutation process. The result of crossover will be two numbers, let this be (k,h) and out of two, one candidate is picked based on the presence of number of ones. The candidate is now allowed for mutation, whose process is explained in the further sections of this paper, the other number is kept as it is without any change. Let the picked candidate be h, and the result of the mutation be v, the result after the process is (k,v).

4. (m,n) is placed in the header and (k,v) is substituted as the trailer and the packet is sent to the CH.

5. The process is repeated by all the ordinary nodes in a network that wants to communicate with the CH. The respective CHs wait until it receives the data from all the ordinary nodes and again follows same procedure as in step 1 to step 4 and places header and trailer information in the packet and sends to the BS.

3.3 Crossover

Let the range received by the higher hierarchy node be (p,q). Select two numbers randomly and let this be (m,n). The step involved is given below:

1. Initially, calculate intermediate number,

$$E = (m+1) + (n-1); \tag{1}$$

2. Find the smallest multiple of 3 between the range (m,E), let this be x, else use m. 3 is an example this can also be made random, and depends on the robustness required.

3. Find $(x\%8)$, which gives the point at which (m,n) has to be crossovered. Here 8 is chosen since the size of keys chosen for communication is 8 bits. The example is shown below.

$Ex:$
$(p,q) = (12,70)$,
$(m,n) = (15,56)$;
$E = (15+1)+(56-1) = 71$;
The smallest multiple between (15, 71) is x= 15;

4. $(15\%8) = 6$; hence 6 is the crossover point. The bits from 6^{th} position to the 8^{th} position of (m,n) is crossovered with one another.

   $m = 15 = 00001111$
   $n = 56 = 00111000$
   After crossover $\rightarrow 00101111 \rightarrow 47$
   $\rightarrow 00011000 \rightarrow 24$

   The result of crossover is $(m,n) = (47,24)$.

3.4 Mutation

The two bytes obtained after the crossover is checked for number of 1's individually and the key with the highest number of ones is chosen as the best candidate for mutation. From the example dealt in the crossover section, the best candidate chosen is 47 because it has more number of 1's in it.

The mutation is carried out in such a way that all the bits in the number are complemented.

$Ex:$
$47 \rightarrow 00011111$
$11100000 \rightarrow 223$

The packet is put with (15, 56) as the header and (47, 223) as the trailer information and sent to the higher hierarchical sensor node.

3.5 Verification at the CH for the packet sent by ordinary node or verification at the BS for the packet sent by CH

1. Start
2. Receive the packet
3. Extract header
4. Check header, whether it is in the range that was sent by itself. **Let the received header be *m, n* and trailer be *k, v*.**

   /*(p,q) range received by the higher hierarchy node*/

   if ($m \geq p$ *and* $n \leq q$) **then**

     /* packet cleared stage-1*/

     (g,h) = Crossover (m,n);

     /*h_1 and h_2 are results of crossover*/

     Select the best candidate for mutation. Let this be x.

     (g_1,h_1)= Mutation (x);

     if ($g_1 == k$ and $h_1 == v$) **then**

       /* packet cleared stage-2*/

     else

       /* packet is malicious*/

     end

   else

   /* packet is malicious*/

   end

5. Stop

3.6 Packet Description

i. Packet sent from BS to CH/ CH to its member nodes

MAC	p	q

where, MAC$\rightarrow$ address of the intended CH node and p, $q\rightarrow$ keys randomly picked.

ii. Packet sent from ordinary node to CH/ CH to BS

This packet consists of the details regarding randomly picked keys by the node and the trailer.

m	n	CRITICAL INFO	k	v

where, $m,n \rightarrow$ keys randomly picked by the node for communication with its CH and g_1, h_1 are the trailers after crossover and mutation, CRITICAL INFO $\rightarrow$ consists of various fields including, preamble, sync bits, destination address, type, group identity, length of message, counter for message sent, source address, error checking bits and payload.

4. Radio Model

The proposed methodology uses a classical radio model [10]. The sensor node is a transceiver. Hence, this radio model gives the energy consumed for the transmission and reception. The block diagram representation is shown in fig. 1. The radio model consists of transmitter and receiver equivalent of the nodes separated by the distance'd'. Where E_{tx}, E_{rx} are the energy consumed in the transmitter and the receiver electronics. E_{amp} is the energy consumed in the transmitter amplifier in general, and it depends on the type of propagation model chosen either free space or multipath with the acceptable bit error rate. We consider E_{fs} for free space propagation and E_{mp} for multipath propagation as the energy consumed in the amplifier circuitry. The transmitter and the receiver electronics depends on digital coding, modulation, filtering and spreading of data. Additional to this there is an aggregation energy consumption of E_{agg} per bit if the node is cluster head.

4.1 Energy Consumption

This section describes the energy consumed for communication.

Packet transmission

$$E_t = (L_P * E_{tx}) + (L_P * E_{amp} * d^n); \qquad (2)$$

where, $L_P \rightarrow$ is the packet length in bits, and $n \rightarrow$ is the path loss component which is 2 for free space and 4 for multipath propagation.
Suppose a node transmits a packet. Each bit in a packet consumes E_{tx} amount of transmitter electronics energy, E_{amp} amount of

amplifier energy. A packet of length L_P, consumes an overall energy of E_t.

Packet reception

$$E_r = (L_P * E_{rx}); \quad (3)$$

where, $L_P \rightarrow$ is the packet length in bits.

Suppose a node receives a packet. Each bit in a packet consumes E_{rx} amount of receiver electronics energy. A packet of length L_p, consumes an overall energy of E_r.

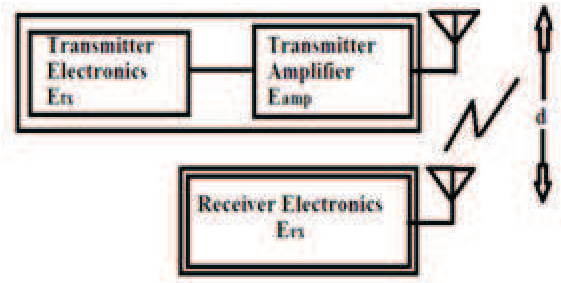

Figure 1. *Radio Model.*

5. Attack Scenario

The system relies on confusing the intruder by randomly varying the keys and ranges chosen for selecting the keys at the BS. The newly deployed malicious attacker may spoof unwanted packets to the CH or the BS. The attack scenarios are shown in the fig. 2 and fig. 3.

The new node carefully listens to the network paradigm and assigns its MAC address with that of another node, of which it may start disguising and spoofing packets to the higher hierarchical node. The packets follow the double verification steps and gets identified itself as either a legitimate or a spoofed packet. Suppose, the count of spoofed packets reaches above a pre-fixed threshold, an alarm is sent to the BS for preventing the further epidemic of the infected packet.

The spoofing can also be done at time by the legitimate nodes already deployed. The spoofing in this case can also be detected by the proposed methodology.

Since, the protocol protects the network using randomization concept, the attack not being identified is minimal. One scenario of attack was modeled in this paper, where a malicious node listens to the paradigm of the network and gets to know about the key ranges i.e. the keys are falling within the range (A, B), and puts header of the packet with those numbers and trailers with some random numbers. In this case, there are chances that the packet may pass the first verification stage, but the second stage clearance is difficult since the numbers in the headers has to undergo crossover, mutation and results has to match with the trailers. The results obtained for this scenario of attack is discussed in the fig. 4, fig. 5, fig. 6, fig. 7 and fig. 8. Apart from this case, if the malicious node has to successfully spoof the packet in every attack, then it has to get the algorithmic and mathematical details burnt in the node, which is the case of a node capture attack. The protocol fails if the node undergoes a capture attack and the security details are hacked.

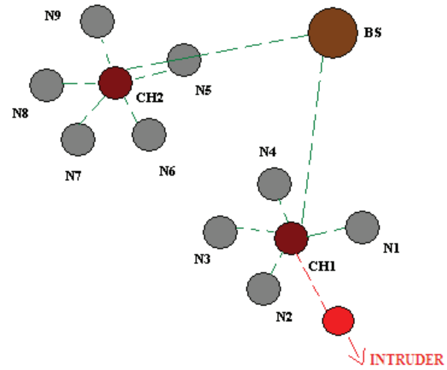

Figure 2. *Malicious ordinary node sending a false packet to CH.*

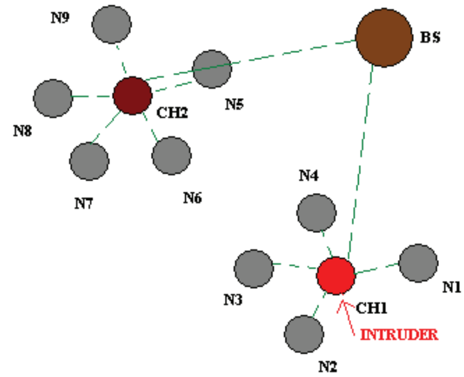

Figure 3. *Malicious CH sending a false packet to the Base Station.*

6. Simulations

The algorithm was executed and tested using MATLAB 2013a on Intel core 5 Duo processor with windows operating system. CH requirement was set to 10% and the algorithm was verified on LEACH protocol till 1000 rounds. Table 1 contains the overhead in packet size due to the proposed security algorithm and table 2 depicts the various key sizes used for simulation. The parameters were set for modeling network environment is shown in table 3. The key sizes of ECC and RSA is shown in table 4, and of which the basic key size of 112 for ECC and 512 for RSA was considered for energy analysis.

7. Results and Discussions

This section deals with the results obtained. The algorithm was tested on LEACH protocol. First five iterations are for analyzing the security, where number of rounds was limited to 100 in every iteration. Next, were five iterations each with 500 rounds. In both cases, after every fifth round a malicious packet was made to spoof into the network, the probability of being identified is

Table 1. *Bits overhead due to cryptographic framework (per communication).*

Parameter	Value
Packet sent from BS to CHs	32 bits
Packet sent from CH to ordinary node	32 bits
Packet sent from end node to CH	32 bits
Packet sent from CH to BS	32 bits

Table 2. *Key sizes used in packets for communication.*

Parameter	Value
p,q	1 byte each
MAC	2 bytes
m,n	1 byte each
k,v	1 byte each

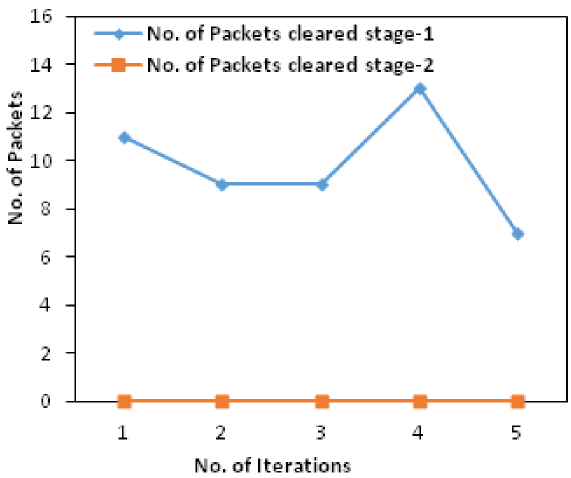

Figure 4. *Number of spoofed packets identified for five iterations (each for 100 rounds of LEACH).*

checked, and the graph is plotted. It was observed that in both the cases, the accuracy in identifying the malicious packets was 100%

Table 3. *Radio characteristics and other parameters chosen for simulation.*

Parameter	Size
Number of nodes	100
Transmitter electronics, E_{tx}	$50nJ/bit$
Receiver electronics, E_{rx}	$50nJ/bit$
E_{mp}	$0.0013pJ/bit$
E_{fs}	$10pJ/bit$
E_{agg}	$5nJ/bit$
Length of plot	$100m$
Width of plot	$100m$
L_{pt}(packet sent from CH to Bs)	$6400bits$
L_{ctr}(packet sent from ordinary node to CH)	$200bits$
Initial energy of the node	$0.5J$

Table 4. *RSA and ECC key length comparison.*

RSA	ECC
512	112
1024	160
2048	224
3072	256
7680	384
15360	512

as per fig.6 and fig. 7. In addition, in both the cases the number of packets clearing first stage and second stage of verification was plotted separately as per the fig. 4 and fig. 5.

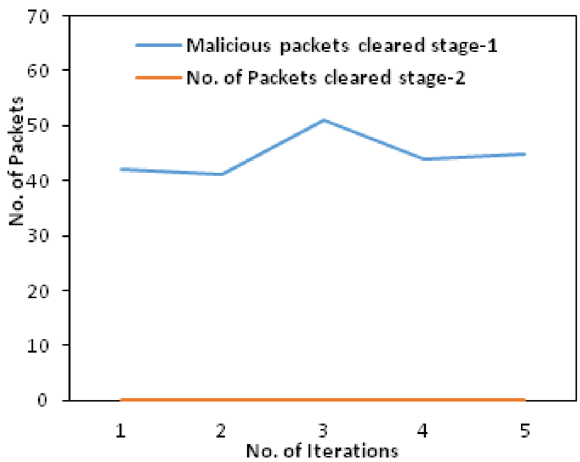

Figure 5. *Number of spoofed packets identified for five iterations (each for 500 rounds of LEACH).*

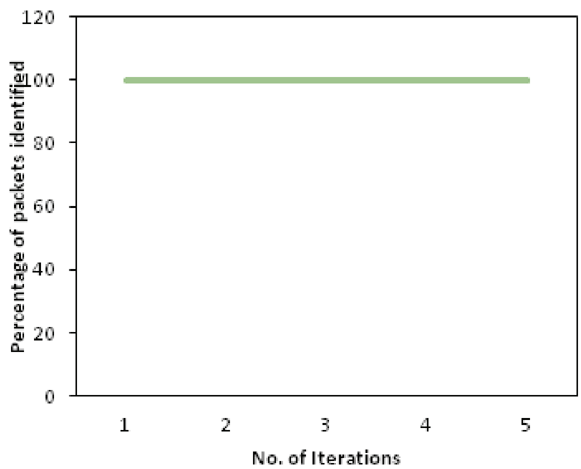

Figure 6. *Percentage of spoofed packets identified (each iteration with 100 rounds of LEACH).*

It was observed that even though the packets clear first stage, it was likely that they were caught in the second stage of verification; hence, the accuracy was always 100% and shows the

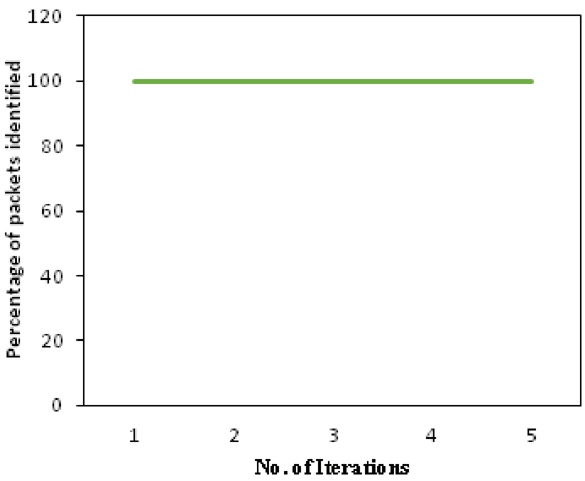

Figure 7. *Percentage of spoofed packets identified (each iteration with 500 rounds of LEACH).*

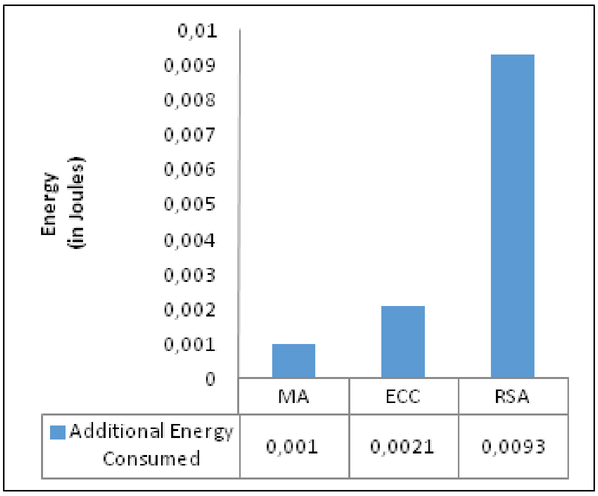

Figure 8. *Additional Energy consumed for 100 rounds between various cryptographic techniques.*

robustness of the protocol in identifying the spoofed packets. The energy consumption analysis of our scheme with the existing cryptographic schemes like ECC and RSA was done for 100 rounds of LEACH for 10% of CH requirement, and the overhead in the energy consumption is plotted in fig. 8.

It was observed that the modeled memetics based algorithm (MA) is more energy efficient than the other widely used keying techniques and the results prove that the technique is robust in providing security in the network.

8. Conclusions

Security in WSNs has always been a difficult task in WSN to address. In this context, memetics based random keying approach is one of the contribution. It was observed a 100% accuracy in identifying the spoofed packets, since every packet has to undergo a double verification stage to get through into the network. In addition, the energy overhead calibration due to the use of the technique gives a promising result compared to other techniques. The developed algorithm uses confusion strategy in combination with memetics for identifying the spoofed packets. The obtained results prove that the algorithm can be implemented in the future networks with an ease.

References

[1] TING, Chuan-Kang et LIAO, Chien-Chih. A memetic algorithm for extending wireless sensor network lifetime. *Information Sciences*, 2010, vol. 180, no 24, p. 4818-4833.

[2] FERENTINOS, Konstantinos P. et TSILIGIRIDIS, Theodore A. A memetic algorithm for optimal dynamic design of wireless sensor networks. *Computer Communications*, 2010, vol. 33, no 2, p. 250-258.

[3] KUMAR, E. Sandeep, KUSUMA, S.M., KUMAR, B.P. Vijaya, A Random Key Distribution based Artificial Immune System for Security in Wireless Sensor Networks, *Proc. of IEEE International Students' Conference on Electronics, Electrical and Computer Science (SCEECS)*-2014, 1-2 March, MANIT, Bhopal, Madhya Pradesh.

[4] KUMAR, E. Sandeep, KUSUMA, S.M., KUMAR, B.P. Vijaya, An Intelligent Defense Mechanism for Security in Wireless Sensor Networks, *Proc. of IEEE International Conference on Communications and Signal Processing (ICCSP)* -2014, 3-5 April, APEC, Melmaruvattur, Tamil Nadu.

[5] SALEEM, Kashif, FISAL, Norsheila, HAFIZAH, Sharifah, et al. An intelligent information security mechanism for the network layer of WSN: BIOSARP. In : *Computational Intelligence in Security for Information Systems. Springer Berlin Heidelberg*, 2011. p. 118-126.

[6] FU, Rongrong, ZHENG, Kangfeng, LU, Tianliang, et al. Biologically Inspired Anomaly Detection for Hierarchical Wireless Sensor Networks. *Journal of Networks*, 2012, vol. 7, no 8, p. 1214-1219.

[7] V RANJITHKUMAR, P., P NEMAGOUD, Sandeep, KUMAR E, Sandeep, et al. A Novel Security Framework based on Genetics for Clustered Wireless Sensor Networks. *International Journal of Computer Applications*, 2014, vol. 96, no 5, p. 8-13.

[8] Concepts of memetics from, Memetics-http://en.wikipedia.org/wiki/Memetics

[9] Concepts of memetics from site nature- inspired algorithms: http://www.cleveralgorithms.com/natureinspired/physical/memetic_algorithm.html

[10] HEINZELMAN, Wendi Rabiner, CHANDRAKASAN, Anantha, et BALAKRISHNAN, Hari. Energy-efficient communication protocol for wireless microsensor networks. In : System Sciences, 2000. *Proceedings of the 33rd Annual Hawaii International Conference on*. IEEE, 2000. p. 10 pp. vol. 2.